REFINE YOUR SEARCH Search Results Related Journals Related Magazines Related SI

Results 1 - 20 of 3,271 Sort by relevance

Result page: **1** 2 3

1 Making secure processors OS- and performance-friendly
Siddhartha Chhabra, Brian Rogers, Yan Solihin, Milos Prvulovic
March 2009 **Transactions on Architecture and Code Optimization (TA**
Publisher: ACM Request Permissions
Full text available: Pdf (1.04 MB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 216, Downl

In today's digital world, computer security issues have become increasi researchers have proposed designs for secure processors that utilize ha and integrity verification to protect the privacy ...

Keywords: Secure processor architectures, memory encryption, memo

2 Design and Implementation of the AEGIS Single-Chip Secure Proce Functions
G. Edward Suh, Charles W. O'Donnell, Ishan Sachdev, Srinivas Devadas
June 2005 **ISCA '05:** Proceedings of the 32nd annual international symp
Publisher: ACM
Full text available: Pdf (288.96 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 106, Downlo

Secure processors enable new applications by ensuring private and auth face of physical attack. In this paper we present the AEGIS secure proc RTL implementation on FPGAs. By using ...

Also published in:
May 2005 **SIGARCH Computer Architecture News** Volume 33 Issue 2

3 Authentication Control Point and Its Implications For Secure Process
Weidong Shi, Hsien-Hsin S. Lee
December 2006 **MICRO 39:** Proceedings of the 39th Annual IEEE/ACM Inte Microarchitecture
Publisher: IEEE Computer Society
Full text available: Pdf (619.30 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 2, Downloads (12 Months): 46, Downloa

Secure processor architecture enables tamper-proof protec- tion on soft

security prob- lems such as reverse-engineering prevention, trusted cor providing a secure comput- ing environment ...

4 Processor virtualization for secure mobile terminals
Hiroaki Inoue, Junji Sakai, Masato Edahiro
July 2008 **Transactions on Design Automation of Electronic System**
Publisher: ACM Request Permissions
Full text available: Pdf (1.53 MB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 24, Downloads (12 Months): 234, Downl

We propose a processor virtualization architecture, VIRTUS, to provide i applications and virtualized domains for downloaded native applications generation mobile terminals can provide ...

Keywords: Multiprocessor, processor virtualization

5 Efficient Memory Integrity Verification and Encryption for Secure Pro
G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas I
December 2003 **MICRO 36:** Proceedings of the 36th annual IEEE/ACM Inte Microarchitecture
Publisher: IEEE Computer Society
Full text available: Pdf (307.01 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 79, Downloa

Secure processors enable new sets of applications suchas commercial g protection,and secure mobile agents by providing security from bothphy paper proposes newhardware mechanisms for memory ...

6 Using Address Independent Seed Encryption and Bonsai Merkle Tre
OS- and Performance-Friendly
Brian Rogers, Siddhartha Chhabra, Milos Prvulovic, Yan Solihin
December 2007 **MICRO '07:** Proceedings of the 40th Annual IEEE/ACM Inte Microarchitecture
Publisher: IEEE Computer Society
Full text available: Pdf (954.09 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 50, Downlo

In today's digital world, computer security issues have become increasi researchers have proposed designs for secure processors which utilize h and integrity verification to protect the privacy ...

7 Fast Secure Processor for Inhibiting Software Piracy and Tampering
Jun Yang, Youtao Zhang, Lan Gao
December 2003 **MICRO 36:** Proceedings of the 36th annual IEEE/ACM Inte Microarchitecture
Publisher: IEEE Computer Society
Full text available: Pdf (258.88 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 89, Downloa

Due to the widespread software piracy and virus attacks,significant effo
security forcomputer systems. For stand-alone computers, a key observ
any component isvulnerable to security attacks. ...

8 Design of secure cryptography against the threat of power-attacks in
Catherine H. Gebotys
February 2004 **Transactions on Embedded Computing Systems (TECS)**
Publisher: ACM Request Permissions
Full text available: Pdf (214.56 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 79, Downloa

Embedded wireless devices require secure high-performance cryptograp
energy dissipation. This paper presents for the first time a design metho
complex DSP-embedded processor core. Elliptic ...

Keywords: VLIW

9 A novel secure wireless video surveillance system based on Intel IXI
Hao Yin, Chuang Lin, Berton Sebastien, Xiaowen Chu
October 2005 **WMuNeP '05:** Proceedings of the 1st ACM workshop on Wire
performance modeling
Publisher: ACM Request Permissions
Full text available: Pdf (399.19 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 51, Downloa

This paper presents the design of a novel high-secure wireless video sui
based on the 802.11g ad-hoc wireless infrastructure; and the Intel IXP4
the basic processing unit. A media-dependant ...

Keywords: ad-hoc network security, network processor, video selectiv

10 Fault-secure algorithms for multiple-processor systems
Prithviraj Banerjee, Jacob A. Abraham
January 1984 **ISCA '84:** Proceedings of the 11th annual international symp
Publisher: ACM
Full text available: Pdf (844.91 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 35, Downloa

In this paper we describe techniques for achieving fault secureness with
systems. In order to do this we consider the relationshipsN between alg

Also published in:
June 1984 **SIGARCH Computer Architecture News** Volume 12 Issue 3

11 Accelerating memory decryption and authentication with frequent val
Weidong Shi, Hsien-Hsin S. Lee
May 2007 **CF '07:** Proceedings of the 4th international conference on Co
Publisher: ACM Request Permissions
Full text available: Additional Information: full citation, abstrac

Pdf (336.57 KB)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 40, Downloa

This paper presents a novel architectural technique to hide fetch latency and authenticated memory. A number of recent secure processor desigr encryption and authentication to protect un-trusted ...

Keywords: message authentication, secure processors, value predictio

12 HIDE: an infrastructure for efficiently protecting information leakage
Xiaotong Zhuang, Tao Zhang, Santosh Pande
December 2004 **ASPLOS-XI:** Proceedings of the 11th international confere programming languages and operating systems

Publisher: ACM Request Permissions
Full text available: Pdf (216.31 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 72, Downloa

XOM-based secure processor has recently been introduced as a mechan resistant execution. XOM provides support for encryption/decryption an XOM nor any other current approach adequately ...

Keywords: address bus leakage protection, secure processor

Also published in:
November 2004 **SIGPLAN Notices** Volume 39 Issue 11
December 2004 **SIGOPS Operating Systems Review** Volume 38 Issue 5
December 2004 **SIGARCH Computer Architecture News** Volume 32 Issue 5

13 Extending hardware based mandatory access controls for memory t
Brian L. Sharp, Gregory D. Peterson, Lok Kwong Yan
May 2008 **CSIIRW '08:** Proceedings of the 4th annual workshop on Cyb intelligence research: developing strategies to meet the cyber challenges ahead

Publisher: ACM
Full text available: Pdf (31.86 KB) Additional Information: full citation, append index terms

Bibliometrics: Downloads (6 Weeks): 26, Downloads (12 Months): 246, Downl

Current memory architectures do not practice the principle of least privi memory to data corruption and usurpation threats, collectively called m famous of such threats is probably the buffer ...

Keywords: data corruption, data usurpation, hardware, mandatory acc safety

14 A low-cost memory remapping scheme for address bus protection
Lan Gao, Jun Yang, Marek Chrobak, Youtao Zhang, San Nguyen, Hsien-Hsi
September 2006 **PACT '06:** Proceedings of the 15th international conferenc

compilation techniques
Publisher: ACM Request Permissions
Full text available: Pdf (536.42 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 25, Downloa

The address sequence on the processor-memory bus can reveal abunda of a program. This can lead to critical information leakage such as encry Addresses can be observed by attaching ...

Keywords: address bus leakage protection, secure processor

15 AEGIS: architecture for tamper-evident and tamper-resistant process
G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas I
June 2003 **ICS '03:** Proceedings of the 17th annual international confere
Publisher: ACM Request Permissions
Full text available: Pdf (286.90 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 142, Downlo

We describe the architecture for a single-chip aegis processor which car secure against both physical and software attacks. Our architecture assi the processor, such as memory, ...

Keywords: certified execution, secure processors, software licensing

16 Hardware authentication leveraging performance limits in detailed sir
Daniel Y. Deng, Andrew H. Chan, G. Edward Suh
July 2009 **DAC '09:** Proceedings of the 46th Annual Design Automation C
Publisher: ACM Request Permissions
Full text available: Pdf (197.10 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 65, Downlo

This paper proposes a novel approach to check the authenticity of hardv performance gap between real hardware and simulations or emulations we demonstrate that each processor design can ...

Keywords: hardware authentication, secure processors

17 A combined hardware and software architecture for secure computin
Jörg Platte, Edwin Naroska
May 2005 **CF '05:** Proceedings of the 2nd conference on Computing fron
Publisher: ACM Request Permissions
Full text available: Pdf (507.25 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 60, Downlo

Remote code execution becomes more and more important as can be se computing projects like SETI@home. However, executing programs on t risks if the program contains sensitive data or ...

Keywords: certified execution, encrypted programs, secure processors

18 Hardware-rooted trust for secure key management and transient trus
Jeffrey S. Dwoskin, Ruby B. Lee
October 2007 **CCS '07:** Proceedings of the 14th ACM conference on Compu
Publisher: ACM Request Permissions
Full text available: Pdf (520.62 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 137, Downl

We propose minimalist new hardware additions to a microprocessor chi portable computing devices which are used in the field but owned by a *architecture* has trust rooted ...

Keywords: emergency response, hardware policy enforcement, key ma secure processors, transient trust

19 Architecture for Protecting Critical Secrets in Microprocessors
Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, Zhengt
June 2005 **ISCA '05:** Proceedings of the 32nd annual international symp
Publisher: ACM
Full text available: Pdf (143.62 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 101, Downlo

We propose "secret-protected (SP)" architecture to enable secure and c secrets for a given user in an on-line environment. Keys are examples c and management is a fundamental problem ...

Also published in:
May 2005 **SIGARCH Computer Architecture News** Volume 33 Issue 2

20 Architectural Support for High Speed Protection of Memory Integrity Multiprocessor Systems
Weidong Shi, Hsien-Hsin S. Lee, Mrinmoy Ghosh, Chenghuai Lu
September 2004 **PACT '04:** Proceedings of the 13th International Conferen Compilation Techniques
Publisher: IEEE Computer Society
Full text available: Pdf (255.33 KB) Additional Information: full citation, abstrac

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 65, Downloa

Recently there is a growing effort in both the architecture and the secur solution for authenticating system memory. As shown in the previous wo authentication will become a vital component for ...

Result page: **1** 2 3